In the Claims

The status of claims in the case is as follows:

1. [Currently amended] A method of operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing, comprising the steps executed at one end of a VPN connection of:

configuring a VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine;

configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

starting said VPN connection;

loading to an operating system kernel at said one end of said VPN connection the security associations and connection filters for said VPN connection;

processing at said one end of said VPN connection a IP datagram for said VPN connection; and

applying VPN NAT at one end of said VPN connection to said IP datagram with source and destination port values after the application of VPN NAT being the same as before application of VPN NAT.

2. [Original] The method of claim 1, wherein said VPN connection is configured for outbound processing, and said applying step comprises outbound source IP Nating.

3. [Original] The method of claim 1, wherein said VPN connection is configured for some combination of inbound processing, and said applying step selectively comprises inbound source IP NATing or inbound destination IP NATing.

4. [Original] The method of claim 1, further for

integration of NAT with IP Sec for manually-keyed IP Sec connections, comprising the further step of manually configuring connection keys.

5. [Original] The method of claim 1, further for integrating NAT with IP sec for dynamically-keyed (e.g. IKE) IP Sec connections, comprising the further step of:

configuring the VPN connections to obtain their keys automatically.

6. [Original] The method of claim 1, further for integrating NAT with IP Sec Security Associations, negotiated dynamically by IKE, wherein said starting step further comprises creating a message for IKE containing said IP address from said NAT pool; and further comprising the step of operating IKE to obtain dynamically negotiated keys.

7. [Original] The method of claim 6, further comprising the step of combining the dynamically obtained keys with said NAT pool IP address and wherein said loading step loads the result as security associations into said operating system kernel.

8. [Currently amended] A computer implemented method for allowing the definition and configuration of NAT directly with definition and configuration of IPsec-based VPN connections and VPN policy, comprising the steps executed by a digital processor at one end of a VPN connection of:

configuring at one end of said VPN connection the requirement for VPN NAT by a yes/no decision in a policy database for each of the three types of VPN NAT, said three types being VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT; [[and]]

configuring at said one end of said VPN connection on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine a remote IP address pool or a server IP address pool selectively responsive to said yes/no decision for each said VPN NAT type; and

upon subsequent start of said VPN connection, processing inbound and outbound packets at said one end of said VPN connection responsive to configuration of said VPN NAT in said policy database and configuration

of said remote IP address pool.

9. [Previously presented] The computer implemented method of claim 8, further comprising the step of configuring a unique said remote IP address pool for each remote address to which a VPN connection will be required, whereby said remote IP address pool is keyed by a remote ID.

10. [Previously presented] The computer implemented method of claim 8, further comprising the step of configuring said server IP address pool once for a system being configured.

11. [Currently amended] A computer implemented method of providing customer tracking of VPN NAT activities as they occur in an operating system kernel, comprising the steps executed at one end of a VPN connection of:

responsive to VPN connection configuration, generating journal records as a log entry in a file system of an operating system at said one end of said VPN connection;

updating at said one end of said VPN connection said journal records with new records for each datagram

processed through a VPN connection; and

enabling a customer to manage said journal records.

12. [Currently amended] A computer implemented method of allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load- balancing, comprising the steps executed by a digital processor at one end of a VPN connection of:

configuring at said one end of said VPN connection a server VPN NAT IP address pool for a system being configured;

storing at said one end of said VPN connection specific IP addresses that are globally routable in said server VPN NAT IP address pool;

configuring at said one end of said VPN connection a VPN connection to utilize said server VPN NAT IP address pool; and

managing at said one end of said VPN connection total volume of concurrent VPN connections responsive to the

number of addresses in said server VPN NAT IP address pool with source and destination port values before and after application of VPN NAT being the same.

13. [Currently amended] A method of controlling the total number of VPN connections for a system based on availability of VPN NAT addresses, comprising the steps executed at one end of a VPN connection of:

configuring on a VPN gateway machine at said one end of said VPN connection employing only IP address data available at said VPN gateway machine the totality of remote IP address pools with a common set of IP addresses, said addresses being configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses; and

limiting at said one end of said VPN connection the successful start of concurrently active VPN connections responsive to the number of said IP addresses configured across the totality of said remote address pools.

14. [Currently amended] A method of performing virtual

private network (VPN) network address translation on selected ICMP datagrams, comprising the steps executed at one end of a VPN connection of:

combining at said one end of said VPN connection IP Security & VPN NAT by detecting selected types of ICMP type packets; and

responsive to said selected types, performing at said one end of said VPN connection network address translation functions on the entire datagram including ICMP data.

15. [Currently amended] A method of performing virtual private network (VPN) network address translation on selected FTP datagrams, comprising the steps executed at one end of a VPN connection of:

combining at said one end of said VPN connection IP Security & NAT by detecting the occurrence of FTP PORT or PASV FTP commands; and

responsive to said command, performing at said one end of said VPN connection network address translation on

the FTP data and the header.

16. [Currently amended] A computer system for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing executed by a digital processor at one end of a VPN connection, comprising:

means for configuring on a VPN gateway machine at said one end of a VPN connection a VPN NAT IP address pool employing only IP address data available at said VPN gateway machine;

means for configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

means for obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

means for starting said VPN connection at said one end of said VPN connection;

means for loading at said one end of said VPN connection to an operating system kernel the security associations and connection filters for said VPN connection;

means for processing at said one end of said VPN connection a IP datagram for said VPN connection; and

means for applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after application of VPN NAT being the same as before application of VPN NAT.

17. [Currently amended] A system for definition and configuration of NAT directly with definition and configuration of VPN connections and VPN policy executed by a digital processor at one end of a VPN connection, comprising:

a policy database for configuring at said one end of said VPN connection the requirement for VPN NAT by a yes/no decision for each of the three types of VPN NAT, said three types being VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN

NAT type d inbound destination IP NAT; and

a remote IP address pool or a server IP address pool at said one end of said VPN connection selectively configured on a VPN gateway machine at said one end of a VPN connection responsive to said yes/no decision for each said VPN NAT type employing only IP address data available at said VPN gateway machine.

18. [Currently amended] A system implemented at one end of a VPN connection for allowing a VPN NAT address pool to be associated with a gateway, thereby allowing server load-balancing, comprising:

a server VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection configured for a given system being configured for containing multiple ~~address~~ addresses configured as a range, as a list of single addresses, or any combination of multiple ranges and single addresses employing only IP address data available at said VPN gateway machine;

said server VPN NAT IP address pool storing specific IP addresses that are globally routable;

a VPN connection at said one end of said VPN connection configured to utilize said server VPN NAT IP address pool; and

a connection controller for managing at said one end of said VPN connection total volume of concurrent VPN connections responsive to the number of addresses in said server VPN NAT IP address pool with source and destination port values after application of VPN NAT being the same as before application of VPN NAT.

19. [Currently amended] A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps executed at one end of a VPN connection for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing, said method steps comprising:

configuring on a VPN gateway machine at said one end of a VPN connection a NAT IP address pool employing only IP address data available at said VPN gateway machine;

configuring at said one end of said VPN connection a

VPN connection to utilize said VPN NAT IP address pool;

obtaining a specific IP address from said VPN NAT IP address pool, and allocating at said one end of said VPN connection said specific IP address for said VPN connection;

starting said VPN connection at said one end of said VPN connection;

loading to an operating system kernel at said one end of said VPN connection the security associations and connection filters for said VPN connection;

processing at said one end of said VPN connection a IP datagram for said VPN connection; and

applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after application of VPN NAT being the same as before application of VPN NAT.

20. [Currently amended] An article of manufacture comprising:

a computer useable medium having computer readable program code means embodied therein for operating a virtual private network (VPN) based on IP Sec that integrates network address translation (NAT) with IP Sec processing executed at one end of a VPN connection, the computer readable program means in said article of manufacture comprising:

computer readable program code means for causing a computer to effect configuring a VPN NAT IP address pool on a VPN gateway machine at said one end of a VPN connection employing only IP address data available at said VPN gateway machine;

computer readable program code means for causing a computer to effect configuring at said one end of said VPN connection a VPN connection to utilize said VPN NAT IP address pool;

computer readable program code means for causing a computer to effect obtaining at said one end of said VPN connection a specific IP address from said VPN NAT IP address pool, and allocating said specific IP address for said VPN connection;

computer readable program code means for causing a computer to effect starting at said one end of said VPN connection said VPN connection;

computer readable program code means for causing a computer to effect loading at said one end of said VPN connection to an operating system kernel the security associations and connection filters for said VPN connection;

computer readable program code means for causing a computer to effect processing at said one end of said VPN connection a IP datagram for said VPN connection; and

computer readable program code means for causing a computer to effect applying at said one end of said VPN connection VPN NAT to said IP datagram with source and destination port values after the application of VPN NAT being the same as before application of VPN NAT.

21. [Currently amended] A computer implemented method for providing IP security in a virtual private network using network address translation (NAT), comprising the steps

executed by a digital processor at one end of a VPN connection of:

dynamically generating at said one end of said VPN connection NAT rules and associating them selectively with manual [[or]] and dynamically generated (IKE) Security Associations; thereafter

beginning at said one end of said VPN connection IP security that uses the Security Associations; and then

as IP Sec is performed on outbound and inbound datagrams, selectively performing at said one end of said VPN connection one or more of VPN NAT type a outbound source IP NAT, VPN NAT type c inbound source IP NAT, and VPN NAT type d inbound destination IP NAT.

22. [Currently amended] The method of claim 1, said VPN NAT IP address pool containing multiple addresses configured as a range, as a list of single address, or any combination of multiple ranges and single addresses.